Legal Constraints on Information Warfare

Mark Russell Shulman

March 1999

7

Occasional Paper No. 7
Center for Strategy and Technology
Air War College

Air University
Maxwell Air Force Base

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	3/1/1999	Research Paper 3/1/1999

4. TITLE AND SUBTITLE
Legal Contraints on Information Warfare

5. FUNDING NUMBERS

6. AUTHOR(S)
Shulman, Mark Russell

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Air University
Maxwell Air Force Base,
Alabama

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited

12b. DISTRIBUTION CODE
A

13. ABSTRACT ***(Maximum 200 Words)***

As societies and economies increasingly rely on electronic telecommunications,they grow more
vulnerable to threats from other computer systems.At the same time,states'military and intelligence
organizations are increasingly developing the capability to attack and defend these assets.As with the
introduction of earlier weapons systems,some would-be users express the belief that the laws restraining
warfare no longer apply.This essay seeks to explain the emerging relationship between technology,
electronic telecommunications and the laws of war In particular this essay seeks to show

14. SUBJECT TERMS
IATAC Collection, information warfare, law, armed conflict

15. NUMBER OF PAGES
35

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UNLIMITED

Legal Constraints on Information Warfare

Mark Russell Shulman

March 1999

The Occasional Papers series was established by the Center for Strategy and Technology as a forum for research on topics that reflect long-term strategic thinking about technology and its implications for U.S. national security. Copies of No. 7 and previous papers in this series are available from the Center for Strategy and Technology, Air War College, 325 Chennault Circle, Maxwell AFB, Montgomery, Alabama 36112. The fax number is (334) 953-1988; phone (334) 953-2384.

Occasional Paper No. 7
Center for Strategy and Technology
Air War College

Air University
Maxwell Air Force Base, Alabama 36112

The internet address for the Center for Strategy and Technology is:
http://www.au.af.mil/au/awc/awecsat.htm

Contents

Disclaimer

The views expressed in this publication are those of the author and do not reflect the official policy or position of the Department of Defense, the United States Government, or of the Air War College Center for Strategy and Technology.

The Author

Mark Shulman was trained as a diplomatic and military historian working under Paul Kennedy at Yale for his BA and in his doctoral work. Along the way, he studied imperialism and the British Empire at Oxford for a master's degree. Then he took a Ph.D. at the University of California, Berkeley, also studying international history and political science. He completed postdoctoral fellowships at Yale and at Gerogetown and taught military history for several years at Yale. Along with his co-teachers Sir Michael Howard and George Andreopoulos, he published *The Laws of War: Restraints on Warfare in the Western World (Yale, 1994),* and then his own book *Navalism and the Emergence of American Sea Power, 1882-1893 (Naval Institute, 1995*). While working at the National Strategy Information Center in Washington, DC, Dr. Shulman began to conduct research on information warfare. From there, he joined the faculty of the Air War College as an associate professor of military and diplomatic history, teaching in the Department of Conflict and Change. He completed the JAG course on law of information operations. Currently, he is completing the JD course at the Columbia University School of Law where he is Editor-in-Chief of the *Columbia Journal of Transnational Law*. He is also an adjunct associate professor of international relations at Columbia's School of International and Public Affairs.

Preface

As societies and economies increasingly rely on electronic telecommunications, they grow more vulnerable to threats from other computer systems. At the same time, states' military and intelligence organizations are increasingly developing the capability to attack and defend these assets. As with the introduction of earlier weapons systems, some would-be users express the belief that the laws restraining warfare no longer apply. This essay seeks to explain the emerging relationship between technology, electronic telecommunications, and the laws of war. In particular, this essay seeks to show how the norm requiring the discrimination between military and civilian objectives may be retained in an era of long-distance warfare. Finally, it presents a model protocol to guide warriors and lawyers in planning or judging the legitimacy of information operations.

Director's Note

In this essay, Mark Shulman explores a set of concepts that are of interest to the Center for Strategy and Technology. The Center is dedicated to research and studies for the broad defense establishment in the selected areas of strategy and technology. In this case, the subject is the relationship between these two fields and the constraints that are established by the law of armed conflict. At the international level, conventions limit how warfare is waged; while at the national level, the law of armed conflict guides and shapes our activities and help states distinguish the warrior from the murderer. To learn how to fight the wars of the future, it is essential that the defense establishment consider how to shape the laws that govem the next generation of wars.

The laws of war always faced two challenges. The first was that war's confrontational nature and tremendously high stakes often frustrated efforts to set reasonable limits on behavior. This is a timeless challenge that became especially acute in the twentieth century. Mechanized and aerial warfare - in conjunction with new militarist ideologies of Nazism and Stalinism - presented particularly difficult challenges for those seeking to preserve the norms of proportionality, discrimination, and humanity. Fortunately, the international community has generated international conventions and war crimes tribunals.

The laws of war currently face a second on-going challenge, which is how to adapt these laws to technological change. This dynamic itself is as old as civilization and predates David's use of a slingshot to kill Goliath. Medieval Europeans faced it when confronted with a crossbow that could fell a knight in full armor. Early modem soldiers and diplomats again faced it when riflemen discovered that they could stop a cavalry charge before it had begun. In the nineteenth century, dumdum bullets were banned as inhumane. Before the twentieth century, however, new systems usually took decades to move from the original notion to the deployment of a working weapon. Meanwhile, new norms developed to govern their legitimate use. In this century, technological change has accelerated. Military research and development is a multi-billion dollar industry rather than the ad hoc enterprise that existed in previous eras. The result is that weapons are developing far faster than international law, and we have every reason to believe that this trend will continue to accelerate in the twenty-first century.

We now face an extraordinary number of changes on all fronts. The stasis of the Cold War has disintegrated. The state-dominated international political system is being undemiined by a myriad of internal conflicts. Weapons systems characterized by the notion of "iron on target" are giving way to the information age of precision, stealth, and electronic telecommunications systems that not only coordinate attacks but can also perpetrate them. Whatever the long-term impact of the so-called information revolution and the revolution in military affairs, we know with certainty that the laws of war are failing to keep up with the changes that have already taken place. Still, we need laws to guide our behavior. But technological change will not wait for the law to adapt. Enemies will not wait for the United States to develop reasonable standard operating procedures. Thus, the law must change faster than ever before unless we want to risk having our own warriors operating in the gray areas where the law is vague. This lack of vision can only harm American interests.

The Center for Strategy and Technology is pleased to publish *Legal Constraints on Information Warfare* in the Occasional Papers series. The Center is committed to publishing the works of individuals in the defense community that examine the interaction between strategy and technology, and thereby help the defense establishment understand the challenges faced by the United States in the twenty-first century.

William C. Martel,
Director

I. Introduction[1]

> *War is an act offorce to compel our enemy to do our will... [A]ttached to force are certain self-imposed, imperceptible limitations hardly worth mentioning, known as international law and custom, but they scarcely weaken it.*[2]
> *-Carl von Clausewitz*
> *War consists largely of acts that would be criminal if performed in time of peace -- killing, wounding, kidnapping, destroying or carrying off other peoples' property. Such conduct is not regarded as criminal if it takes place in the course of war, because the state of war lays a blanket of immunity over the warriors. But the area of immunity is not unlimited, and its boundaries are marked by the laws of war.*[3]
> *- Telford Taylor*

As Telford Taylor notes, the laws of war distinguish soldiers, sailors, marines, airmen, and even spies from murderers, kidnappers, and arsonists. The distinction Taylor describes is inextricable from legal notions of war, a conclusion down-played or possibly misconstrued by military analyst Carl von Clausewitz in the cited excerpt from his seminal treatise, On War4 In reality, the laws of war have long restrained its legitimate conduct. These constraints include distinctions between campaign and non-campaign seasons,[5] and they guide "the selection of methods, of weaponry and of targets.,,[6] They provide specific immunities for certain persons and places. They distinguish between combatants and noncombatants, between legitimate and illegitimate targets.[7] Over the millennia and particularly the past half-century, these rules have expanded and been codified in international law. Despite remarkable progress, discrimination between legitimate and illegitimate weapons, methods, and targets has also eroded over the past half-century, as warfare expanded from limited set-piece encounters into virtually unlimited wars between multi-state alliances.[8] In addition to the concept of unlimited warfare, there has been a technological revolution that. has changed and will continue to change warfare at an accelerating rate. Even so, this critical norm of humanitarian law has survived. As the laws grew stronger, breaches became more stark.

This essay analyzes some of the problems and suggests some guidelines for retaining discrimination in the era of long-distance, impersonal, and undeclared war in the information age. Section I introduces the topic and laws of war, including the long-standing norm requiring that military planners and operators distinguish between legitimate military objectives and non-combatants. Section II grapples with the fast-changing subject of warfare in the information age. Section III tackles the problems of applying discrimination today. Discrimination faces many new challenges, but the traditional means for formulating solutions still offer valuable tools for finding legal and ethical constraints on the application of force through electronic media. Section IV provides a model protocol that acknowledges these international norms and formalizes them in international law. Then it offers a few concluding remarks.

While states frequently engage in armed conflict,[9] aggressive international war has been outlawed - first by the Kellogg-Briand Treaty and more formidably by the UN Charter.[10] Nonetheless,

> *the application of the laws of war does not depend upon the recognition of the existence of a formal state of 'war', but (with certain qualifications) comprehends situations of armed conflict and military occupation in general, whether formally recognized as 'war, or not.*[11]

Thus the tradition of the laws of war has evolved into the law of armed conflict CLOAC].[12] The applicable law might preferably be called "international humanitarian law applicable in armed conflicts" or "Operational Law."[13] This essay, however, retains the older term "LOAC," as the widely accepted successor body of law to the traditional laws of war. Moreover, because the laws limiting a state's entry

into hostility are now governed by a variety of international laws that have replaced the just war tradition [*jus ad bellum*], this essay will concentrate on the jus in bello -- restraints on the conduct of warfare.

II. Information Warfare

The information revolution based on electronic communications, computers, complex software and the creation of a world-wide web has had dramatic impact on the face of war. The effect of this technology has been to change not only the battlefield but the players involved and the types of targets selected. Ultimately, it is likely to change the rules governing military operations. In the meantime, advances in military technology have out-paced change in the law of armed conflict. This essay attempts to focus on the development of a new type of military and the challenges it poses for the legal regimes that constrain warfare.

The fastest developing type of "armed conflict" is Information Warfare [hereinafter IW]. Ironically, IW is neither 'armed' in the traditional sense, nor does- it necessarily involve 'conflict.' Dramatic hypothetical accounts of IW abound and best serve to introduce this little-known realm. Consider a few hypotheticals. Special forces detonate a small non-nuclear electromagnetic pulse weapon [EMP] near a nation's central bank computer storage facility, destroying the electronic systems that transact, communicate, and archive the nation's financial information. Or an intelligence operator hacks into a nation's telecommunications network, planting a computer code that destroys the software running that system. Or a military operator feeds into another state's television broadcast "morphed" images of that state's religious leader engaged in sacrilegious acts. Or another operator hacks into a target nation's computer network coordinating air or rail traffic to reprogram the systems to shut down without warning.[15]

At the extreme, each of these hypothetical examples would lead to dramatic results: economies could be destroyed; societies disintegrate; planes and trains crash. As a result, governments would fall. Thousands of people would perish. As dramatic as these hypotheticals are, IW may prove complicated and possibly even more devastating than these examples suggest. [16] If subtle or carefully played, attacks may go undetected. For example, an air-traffic controller will wonder why his system crashed at such an inopportune moment. A banker may wonder about a million dollar discrepancy in a large transaction. Radicals seeking to incite their countrymen to genocide may find their radio broadcasts jammed. IW's potential impact ranges from the cataclysmic to the trivial. And yet, we have only begun to consider what it is and how it may be pursued.

Definitions of this fast-changing and mostly classified set of capabilities and operations - IW - vary. Each of the U.S. military services is currently engaged in studying IW. Each has considerable experience and expertise in information operations of one variety or another.[17] Because the Air Force [USAF) appears to be the lead agency, this essay adopts its definitions. IW is any "action to deny, exploit, corrupt, or destroy the enemy's information and its functions; protecting ourselves against those actions; and exploiting our own military information functions."[18] It includes electronic warfare, military deception, physical destruction, security measures, and information attack. [19] The Air Force defines information in this context as "data and instructions" and distinguishes IW from warfare in the information age as those attempts to influence the information directly.[20] This definition is useful not only because the USAF has adopted it but also because it appears to describe the emerging reality. But to really understand IW, it must also be fit into a broader context of military capabilities.

IW operations present a panoply of military capabilities. To illustrate their range, traditional technologies provide useful analogies. While wars of aggression are outlawed by the UN Charter and other binding formulations of international law, the Charter does acknowledge that nothing "shall impair the inherent right of individual or collective self-defense if an armed attack occurs."[21] Some defensive measures are still military operations that bear many of the characteristics of war. At the most basic level, it is important to distinguish between a defensive operation based on an "offensive-defense" and one based on a "defensive-defense.,,[22] For example, the defensive can be offensive, as it was when the Allied Forces landed at Normandy in 1944 or in Kuwait and Iraq in 1991.[23] These are offensive measures undertaken to defend one's national interests. The defense was defensive when the Anglo-French forces

attempted to keep the Wehr7nacht from pushing them out of France in 1940 or when the UN Forces sent USAF F-15s to Saudi Arabia fifty years later to deter the Iraqi invasion. Strictly defensive or security operations include camp or perimeter defenses like sentries filing sidearms when they detect a perimeter breach.

In IW, these distinctions also apply. Offensive-defense IW operations might include 1) active gathering intelligence about information systems;[24] 2) unauthorized intrusions into information systems; 3) introduction of vulnerabilities into information systems; 4) corruption or denial of data; 5) and disabling or destroying information systems.[25] These are sometimes referred to as "information operations." United States law requires that the armed forces and intelligence services of the United States undertake this type of operations only against particular foreign opponents under executive order, presumably as part of a coordinated national policy to implement unilateral or multilateral defensive operationS.[26]

The legal issues of offensive' information operations have never been brought before U.S. courts. However, the military and intelligence agencies could be authorized to undertake them when ordered by the Executive branch. This law has not yet been pled or decided, but it seems like a small step from traditional forms of covert action to the types of IW considered in this essay. The Central Intelligence Agency [CIA] and the Department of Defense (DOD) are granted authority to undertake covert action at the direction of the National Security Council.[27] The breadth of this authority was clarified by Executive Order 12,333 (1981) which provides in part:

> *No agency except the CIA (or the Armed Forces of the United States in time of war declared by Congress or during any period covered by a report from the President to the Congress under the War Powers Resolution (87 Stat. 855)) may conduct any special activity unless the President determines that another agency is more likely to achieve a particular objective.*[28]

Michael Reisman and James Baker convincingly conclude that the "unless" clause "effectively leaves the matter up to the President." [29]

As with the more traditional forms of covert action,[30] however, the particular operations are constrained by LOAC in addition to requiring executive authorization. As with all operations, the choice of tool or weapon is critical for the legitimacy of the operation. While the effects of many of these operations could be achieved with conventional arms and various technologies, this essay concentrates on those undertaken via the electronic telecommunications media. Using an explosive on a computer server or a hydroelectric dam, using a radio frequency weapon to destroy a telephone line, or using an electromagnetic pulse [EMP) to disrupt a satellite's operations have enough similarity to conventional warfare that the traditional LOAC would still apply. While not simple, these scenarios do not present new categories of challenges like the type under analysis here. This essay concentrates on information attacks, those that seek to alter "information without visibly changing the physical entity within which it arises."[31] Rather than explosives, lasers, or directed EMP'S, it analyzes the use of such weapons as electronic viruses, worms, and logic bombs. They may be inserted remotely via various media of electronic communications: telephone, radio, or internet. Alternatively, like a clipper chip, they may be embedded in the software of electronic machinery manufactured in the United States and sold abroad.[32] Then they would be triggered remotely by telephone, radio, or other electronic means. These weapons may also be used against the resources, people, or infrastructure of the United States.

If a non-U.S. party (whether state, group, or individual) assaults or attempts to assault a U.S. information system, numerous possible responses exist. As with other forms of armed conflict, defensive-defense IW operations are subject to the restraints of proportionality. The traditional laws of armed conflict provide a starting point for most analysis. Any U.S. response to an attack should be intended to have an effect of inflicting roughly the same scale of harm as was intended in the initial assault. Under general LOAC principles, usually the defensive system should retaliate only against the actual source of that initial assault (or attempt). Application of this general rule is relatively simple when air defense interceptors or missiles shoot down an intruder reconnaissance planes after a failed attempt to warn them

off. It is equally straightforward when a navy destroyer returns fire and sinks an attacking gunboat. IW complicates the equation, because the attacker may not be a single, readily-identified individual.

In a conventional assault, the defender knows precisely who is attacking, e.g. the reconnaissance plane or the gunboat. He may not know its nationality, but he will know which people are directly engaged in the assault. In IW, and assault will likely be camouflaged. The assailants will probably route their assault through a innocent intermediary telecommunications systems. For example, hackers would first route their communications through various servers around the world before attempting to gain access to a U.S. Department of Defense computer system. In such a situation, a too hasty defender might be likely to destroy the innocent system(s) in the effort to thwart and punish the attacker.

A second major distinction is that in a conventional assault, the gravity of the threat is relatively unambiguous. Thus, we know that a reconnaissance plane could collect sensitive information and that a gunboat could sink a cruiser. An electronic assault, however, may merely amount to the hapless intrusion of an American teen-age hacker,[33] for example, or it may be part of a Hazbollah strategy to degrade CENTCOM's command and control functions in preparation for a coordinated large-scale terrorist attack upon Israel.[34] In the months leading up the Gulf War, private Dutch hackers pillaged DOD computers sites and subsequently offered information about UN troops strength, capabilities, and positions to Iraqi leaders.[35] Had Iraqi President Saddam Hussein availed himself of this information, thousands more people on both sides could have died.

The DOD's computers are subject to approximately a quarter of a million such intrusions annually.[36] Any active response must be made carefully

not automatically. An operator "in the loop" would be the person who evaluates the situation, concluding that there has indeed been an attack and deciding what the appropriate response should be. This supervision assures some level of protection for harmless trespassers (children or those entering by mistake). For any decision to use an "active defense system should take into account any information about intruder's skill, status, and apparent intentions.,,[37] These active defense systems can destroy the computers or systems used to launch the assault, or they may go further and destroy the assailant's infrastructure, e.g. the power and telecommunications grids. Removing the human being from this decision (i.e. leaving it to a computer's automated response mechanisms) would likely result in faster but less responsible decisions.

International law traditionally distinguishes between retorsion and reprisal - a valuable distinction that should be retained in the context of information operations. Retorsion consists of an unfriendly but legal act of force undertaken with retaliatory or coercive purpose.[38] Reprisals are more complicated. They involve acts that would be illegal unless they follow three steps. First, there must be an illegal act by another state. Second, the state intending to effect the reprisal must give the original assailant the opportunity to "make right their international wrong." Finally, if this demand goes unsatisfied, then the attacked party may respond in a manner proportional to the original attack.[39]

In the context of IW, the decision to adopt a policy of retorsion or reprisal presents serious but not necessarily fatal @evidence of problems.[40] The likelihood of a camouflaged assault means that the responding parties have no reasonable expectation that they will be punishing the perpetrator, unless they can first trace the assault back as far as a suspect nation, group, or individual. Accordingly, they might limit these forceful responses to those occasions when the assault is traced back to groups or actors on counter-terrorism watch lists. Even then, he may only know that he has traced the attack back to a suspect group. He will likely not know for sure that he has identified the true assailant. So he must proceed with caution. On-screen warnings are important to put intruders on effective notice, although they may be ineffective when intruders gain access through back doors, ie. bypassing entry procedures and access protocols available to legitimate intemet traffic.[41] Additionally, they may evoke false assumptions of guilt, leading to attacks upon the intermediaries who are on the watch list but innocent of the assault. Given these problems, reasonableness suggests that retorsion would be limited to shutting down (either temporarily or permanently) the computer system thought to be the one from which the original attack

was launched. Retorsion would not extend to destroying the power and telecommunications grids in the city of the suspected assailant. This would probably exceed the limits of action deemed defensive-defense.

Strictly defensive operations like computer security [COMPUSECI apply to military and non-military systems alike. Stock exchanges, corporations, travel and communication systems, and educations institutions all rely on the integrity and smooth-running of their own information systems much as the military does, although the failure would rarely be a matter of life and death. Security measures include: virus checks, fire-walls, passwords, or simply locking the building's front door. U.S. domestic losses to hack attacks were estimated at $ 1 00,000,000 in 1995.[42] Estimates for computer fraud of all varieties in the United States run to ten billion dollars a year.[43] Strictly defensive measures must always be applied when protecting critical infrastructure. If not, the society risks losing use of its military, transportation, communications, or other instrumentalities vital to its continued security and well-being.

In terms of military targeting, infrastructure is neither per se military nor civilian. In terms of defense, the United States considers it both.

> *Infrastructure is the framework of interdependent networks and systems comprising identifiable industries, institutions, and distribution capabilities that provide a continuous flow of goods and services essential to the defense and economic security of the United States, the smooth functioning of government at all levels, and society as a whole.*

Furthermore "[c]ertain national infrastructures are so vital that their incapacity or destruction would have a debilitating impact on the defense or econon-dc security of the United States." These include telecommunications, electrical power, gas and oil storage and transportation, banking and finance, transportation, water supply, emergency services and government services.[45] Protecting them is vital to the well-being of the nation.

A myriad of federal laws and enforcement systems provide a strictly defensive defense. Foremost among these laws are the Computer Fraud and Abuse Act and the Wiretap Act, each of which defines felonies and misdemeanors.[46] U.S. law against hacking is broad-ranging and appears comprehensive (within the limits of prosecutorial discretion and some loopholes not relevant to the scope of this essay). Section 1029 of 18 U.S.C. generally prohibits fraud and related activity with telecommunications access devices. The Computer Fraud and Abuse Act, 18 U.S.C. § 1030, is the main hacker law, enumerating the crimes of computer espionage. 18 U.S.C. 1030 prohibits: (a)(1) unauthorized access to computer-based financial records, (a)(2); and unauthorized access to nonpublic computers of a department or agency of the United States, (a)(3); unauthorized access to a computer with intent to defraud, (a)(4); criminal trespass that results in damage, (a)(5); and trafficking in a password, (a)(6). The Wiretap Act makes it unlawful for "any person" to "intentionally intercept, use, or disclose or endeavor to intercept, use, or disclose any wire, oral, or electronic communication" 18 U.S.C. § 251 1. Section 2511 is subject to several exceptions, most importantly for systems administrators, 18 U.S.C. §2511(2)(a)(i); with consent of a party to the communication, §2511(2)(3); or if intercepted under a court order, §2511(2)(a)(ii). The agencies charged with enforcement responsibilities are criminal investigated units of the military services, the intelligence community, and the FBI.[47] Aside from tightening some loopholes, these laws do not appear to need any significant modifications at this point - at least insofar as they seek to protect U.S. infrastructure from IW attacks. In stark contrast, international law is vague and has considerable room for improvement.

III. Discrimination and the Laws of Armed Conflict

Discrimination between military and civilian targets remains imperative in the age of IW - despite the new difficulties of distinguishing legitimate targets within the critical infrastructure. The Geneva Conventions of 1949 memorialized the basic ground rules for warfare.[48] The 1977 Protocol I to the Geneva Conventions established the "Basic Rule" on discrimination which remains valid, if somewhat more difficult to apply to the facts of IW.

> *In order to ensure respect for and protection of the civilian population and civilian objects, the Parties to conflicts shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct operations only against military objectives.* [49]

Article 51 protects civilian populations, and 51(4) defines unlawfully indiscriminate attacks:

> *(a) those which are not directed at a specific military objective; (b) those which employ a method or means of combat which cannot be directed to a specific military objective; or (c) those which employ a method or mean of combat the effects of which cannot be limited as required by this Protocol; and consequently, in each case, are of a nature to strike military objectives and civilians without distinction.*[50]

Even read within the context of Protocol I's Part IV on Civilian Population, this may appear to be self-reflective or even meaningless protection, but it has been given flesh. As the International Court of Justice [51] recently held, this regime does not by itself preclude operations that have a secondary or collateral impact on civilians as long as the intended target is an armed force or other military objective.[52]

The protocol also defines armed forces as Article 43 further fleshes out the basic rule, defining

> *[t]he armed forces of a Party to a conflict [as] all organized armed forces, groups, and units which are under a commander responsible to that Party for the conduct of its subordinates, even if that Party is represented by a government or an authority not recognized by an adverse Party.*[53]

These are the parties for whom the prohibitions apply, prohibiting them from using force to harm non-military objectives and acknowledging them as legitimate targets for lawful attacks. Article 52(2) then defines military objectives as those objects:

> *which by their nature, location, purpose, or use, make an effective contribution to military action and whose total or partial destruction' capture, or neutralization, in the circumstances ruling at the time, offers a definite military advantage.* [54]

These legal definitions, however, only get one to the questions, not the answers. Distinguishing legitimate targets still requires a context with which to test the facts.

The traditional tools for distinguishing civilian from military personnel or operators are not as readily available as they were before the advent of long-range bombardment and telecommunications.[55] Over the three centuries between 1648 and 1945, combatants generally wore uniforms that visibly distinguished them from noncombatants before the engagement.[56] Likewise, most warfare has involved physical proximity. Whether using a sword or a projectile, most combatants could see each other and distinguish combatants from noncombatants. The major exception here is aerial bombardment by airplane or missile.

Even then, those airmen doing the targeting still bore the burden of making realistic distinctions -an obligation unfortunately honored only in the breach.[57]

Whether they are wearing military uniforms or not is inconsequential when the parties cannot see each other. The person launching a computer virus to attack an American military communications system, for example, may be sitting in a basement of a publicly-traded telephone company wearing a bishop's miter. Instead of a military uniform, he would be wearing the symbol of clergy - a protected group sitting in a privately-owned building also doubly protected by being private and vital to the well-being of society. This individual would nonetheless be a combatant subject to a proportional response, such as the destruction of the computer or the local area network. In IW, there is no physical proximity to permit distinguishing combatants from non-combatants visually. Moreover, in IW, the individual is a combatant and subject to proportional response.

Despite these differences, three traditional principles remain valuable for discrimination. These are: military necessity, humanity, and chivalry. Under customary international law, military planners must balance all three.[58] Under U.S. law, military officers must be taught to grapple with these issues.[59] They are also critical for the legitimate undertaking of IW. First, the principle of military necessity demands that "[o]nly that degree and kind of force not otherwise prohibited by the law of armed conflict, required for partial or complete submission of the enemy with a minimum expenditure of time, life, and physical resources may be applied."[60] Military necessity is a complicated argument in an era of one superpower. The United States has at its disposal a vastly greater variety of military and political tools than any other state, past or present. For the United States, therefore, military necessity cannot mean that an act is strictly necessary. For the foreseeable future at least, there will almost always exist alternatives that could not reasonably be measured against each other (i.e., conventional or information operations, economic or diplomatic sanctions, etc.). Nor are there many states that can plausibly threaten the existence of the United States. That said, questions of military necessity in IW do not seem different from those involved in deciding whether to undertake traditional operations. Instead, they focus more on targets and objectives than means. To this extent, IW does not substantially after the decision-making process.

Second, the military planners must weigh the humanity of their actions. Unnecessary suffering and destruction of humanity must be avoided - a universal principle expressed in the Martens Clause of the 1907 Hague Convention, IV. The

> *inhabitants and the belligerents remain under the protection and the rule of the principles of the law of nations, as they result from the usages established among civilized peoples, from the laws of humanity, and the dictates of the public conscience.* [61]

No mere historical footnote, the Martens Clause is embodied in an article common to each of the four 1949 Geneva Conventions. They note that the fact of denouncing the Convention

> *shall in no way impair the obligations which the Parties to the conflict shall remain bound to fulfil by virtue of the principles of the law of nations, as they result from the usages established among civilized peoples, from the laws of humanity and the dictates of the public conscience.*[62]

The notion that humanity remains an underlying principle restraining armed conflict has been embraced and codified in U.S. LOAC.[63]

As with military necessity, humanity in armed conflict is a relative value. It might favor an IW operation, for example, when the only military alternative is dropping a large explosive on or near the same target. On the other hand, it might halt an information attack that would disable the computers controlling not only air defense but also civilian aviation of an automated subway system. Clearly, humanitarian principles prohibit the Sherman-esque logic that reasons "war is cruelty... the crueller it is,

the sooner it will be over."[64] The principle of humanity appears to militate toward information operations if the alternatives threaten greater physical destruction and loss of life.

Third, planners and operators remain bound by the enduring if amorphous principles of chivalry. In many societies this might mean distinguishing between male and female targets, despite the various treaties and national laws banning distinctions based on sex alone.[65] Leaving aside distinctions based on sex, chivalry still protects the young, old, and helpless even beyond the consideration given all noncombatants. Chivalry also bans treachery or perfidy. The 1977 Geneva Protocol I bans "[A]cts inviting the confidence of an adversary to lead him to believe that he is entitled to, or is obliged to accord, protection under the rules of international law applicable in armed conflict, with intent to betray that confidence.,,[66] Perfidy includes: 1) feigning of intent negotiate or surrender, 2) feigning incapacitation, 3) feigning civilian, noncombatant status, and 4) feigning protected status by use of signs or uniforms of the LJN or neutral states. On the other hand, ruse of war is not prohibited, which requires drawing yet another fine distinction under sometimes urgent circumstances.[67] Legitimate ruses include camouflage, decoys, mock operations, and misinformation.

Applying these principles of chivalry in a post-modem conflict seems daunting. But the differences now are more about cultural change than about the employment of particular weapons systems. Military strategist Edward Luttwak believes chivalry is no longer relevant because it is an atavistic throw-back to a more romantic era of warfare. [68] And yet, while chivalry may seem archaic today, it retains some clear normative value. While neither courts nor legislatures have ruled, analogy strongly weighs against that sending an e-mail messages carrying a logic bomb disguised as e-mail from the International Committee of the Red Cross [ICRCI or even from "Microsoft Support" - where such a message might be permissible without labels.[69] Using ICRC and Microsoft tags would constitute an illegitimate act of perfidy, much as would disguising any dangerous military intruder in the form of an innocuous invitee. Chivalry does not, however, appear to ban many other types of clandestine entry into the opponent's system, for instance through trap doors, or by camouflaged instructions from an ally.

In many instances, chivalry may not weigh heavily in the decision to undertake IW, if only because the penalty for underestimating it is not likely to be applied unless the perpetrators lose the war, and thus the evidence and forum that is necessary to convict the individual of a war crime. It is difficult to imagine a realistic penalty for the espionage-like offense of gaining access to a computer by pretending to be one of the penetrated-party's own military personnel. Traditionally, spies may be executed if local law permitS.[70] (But if the spy returns home, then that individual is safe.[71] In IW, the spying may occur from the safety of a windowless office in Fort Meade or Shaw AFB, headquarters of the National Security Agency and the Air Force's IW center respectively. They are already at home and thus safe. Chivalry, therefore, will play only a minor role in IW.

While it is important to weigh military necessity, humanity, and chivalry, some categories of impermissible activities present themselves when the possibilities of IW are applied to the long-standing basic rule of discrimination. For "the rights of belligerents to adopt means of injuring the enemy are not unlimited.,,[72] Nonetheless, the planner may still balance the factors of military necessity, humanity, and chivalry to decide whether the targets are truly impermissible. At one extreme are legitimate targets - military objectives such as army bases, ships of war, weapons depots, and intelligence headquarters. That is not to say that these may all be destroyed for any or no reason. The principles of jus ad bellum, proportionality, military necessity, chivalry, and humanity continue to constrain the treatment of enemy combatants and other military objectives. At the other extreme of the spectrum are those objectives that are strongly protected by international law. Outside the per se categories, there remains a large intermediate area where reasonableness demands weighing military necessity, humanity, and chivalry as well as proportionality. First this essay will address the per se categories and then discuss the more questionable targets.

For nearly a century, certain categories of objects have traditionally been beyond the reach of lawful attack. The Hague Convention on Land Warfare requires that:

In sieges and bombardments all necessary steps must be taken to spare, as far as possible, buildings dedicated to religion, art, science, or charitable purposes, historic monuments, hospitals, and places where the sick and wounded are collected, provided that they are not being used at the time for military purposes.

However, to prevent the rule from being abused to protect otherwise legitimate targets, the convention further demands segregation. "it is the duty of the besieged to indicate the presence of such buildings or places by distinctive and visible signs, which shall be notified to the enemy beforehand."[73] As detailed in the Convention for the Protection of Cultural Property, these include civilian hospitals, cultural, historical, or religious sites, reservoirs of dangerous forces (including dams and nuclear power plants), food and other supplies necessary for human life.[74]

During the most recent large-scale international armed conflict, the Persian Gulf War of 1990-91, Iraq abused these constraints. Among other transgressions, the Iraqi leadership hid military intelligence operations beneath children's milk processing plants and placed military aircraft amidst cultural artifacts.[75] President Saddam Hussein had constructed dozens of statues of himself that were placed among otherwise legitimate targets. This left planners with the dilemma of deciding if the statues were "cultural property" deserving the protection of the Convention. With each of these acts, Hussein flouted his obligation as a defender to segregate military from civilian objectives. In other words, Hussein abused the laws of war, casting the legitimate activities of the Allies in a light of illegitimacy before the CNN court of world opinion. In the future, these cynical games may undermine a state's willingness to risk its own forces in order to adhere to the principle of discrimination as between legitimate and illegitimate targets.

Nonetheless, as the state with the greatest interest in strengthening international humanitarian norms, the United States should continue try to restore discrimination and the defender's obligation to segregate. IW may facilitate this restoration, or at least make it easier for the United States. For instance, if undertaken cautiously, IW may allow the United States to disable certain targets that would be protected from more destructive forms of attack. Thus, while the United States could possibly attack information systems within protected sites with an impact that may not rise to the level of destruction that the conventions prohibit. An IW attack could put out of combat an Iraqi intelligence center, instead of using 2,000-pound bombs to destroy it and the children's shelter beneath it. Likewise, destroying a dam is generally prohibited by Protocol I.

Works or installations containing dangerous forces, namely dams, dykes and nuclear electrical generating stations, shall not be made the object of attack, even where these objects are military objectives, if such attack may cause the release of dangerous forces and consequent severe losses among the civilian population.[76]

Additionally, the Protocol makes it prohibited to

attack, destroy, remove, or render useless objects indispensable to the survival of the civilian population .... for the specific purpose of denying them for their sustenance value to the civilian population or the adverse party, whatever the motive.[77]

On the other hand, temporarily disabling the dam's electronic control system would not be illegitimate if doing so did not unleash a torrent or deprive civilians of water for the purpose of denying them its sustenance. Presumably, the Protocol seeks to avoid the horror of unleashing dangerous forces in a way that would harm civilians. It does not seek to ban outright the denial of a dam's energy or even of its water to an enemy. Here IW would be more flexible and useful tool than explosives which would likely release the deadly forces - or permanently deprive the civilians of drinking water.

Likewise, information warfare may enable operators to disengage a regional electric grid temporarily where they would be prohibited from destroying it. The Hague regime prohibits the "attack or bombardment, by whatever means, of towns, villages, dwellings, or buildings which are undefended."[78] This does not mean that an information warrior can attack a village's power grid or telecommunications network intentionally, justified merely by the fact that the grid or network has some electronic defenses.[79] However, because the village's infrastructure is tied into a regional or national network that is defended by the military, they may be damaged as collateral effects in an information strike on a military target. This impact, however, is likely to be far less serious under an IW attack which only puts it out of commission temporarily, compared to an explosion that would kill people and cause damage that takes more money, time, and resources to repair. Thus IW might permit operations against targets that are generally protected by international conventions. As such, it would not undermine those agreements but further strengthen the conventions by aligning military means to their desired outcomes.

As noted above, for civilians and civilian objects to merit discrimination, the defender has an obligation to segregate them from military objectives. Protocol I requires: "to promote the protection of the civilian population from the effects of the hostilities, combatants are obliged to distinguish themselves from the civilian population while they are engaged in an attack or in a military operation preparatory to an attack.„[80] This obligation is relatively straightforward where armed forces move by military vessels alone. Now most states rely on their civilian infrastructure almost entirely to move large numbers of troops; highways, railroads, and frequently airports are not duplicated by solely military systems. Moreover, armed forces once communicated among themselves via military media: couriers, runners, pigeons, military walkie-talkie, or unsecured telegraph or telephone lines. This shift compels an attempt to compare moving munitions by truck to moving them via telecommunications media.

In the information age, military operations are increasingly reliant upon advanced communications; information and critical infrastructure is shared, frequently gutting the defender's reasonable ability to segregate the military from the CiVilian.[81] Modern Military forces rely on mixed use telecommunications media including telephones, faxes, and e-mail that travel over the civilian owned or operated networks. Even with the unmatched material wealth of the United States, ninety-five percent of all DOD telecommunications traffic flows over public networks. If the wealthiest nation does not have the resources to segregate its command and control systems from the civilian communications network, then one would not expect the remainder of the world to do so.

Deciding whether to destroy civilian communications systems, therefore, requires careful balancing. However, the scale has never materialized. If the measure is lives saved, then IW offers great possibilities for expanding the realm of legitimate targets, because it enables operators to target systems for quiet disablement, rather than the explosive destruction that is more likely to bring excessive collateral damage. To this extent, patterns of legitimate usage should develop as they have for other precision weapons. The USAF

apparently believes the correct formula should be that the attack must be likely to produce a military advantage that outweighs the civilian casualties and damage.[83] This demands weighing the importance of navigation systems, communications systems, and electrical grid systems to the opponent's military effort.[84] It appears to beg the question of how to value these systems. Does one measure in lives saved or lost; dollars spared, saved, risked; or only in permanent physical destruction? IW offers a theoretical opportunity that conventional weapons do not; degrading a system could be reversible in ways that physical destruction could not. This means that lives could be saved while the systems become inoperative, either permanently or briefly. Does this therefore mean that reversible attacks will be launched against civilians or civilian infrastructure more freely? Maybe. Does it strengthen adherence to the norms of discrimination? If the goal is to protect civilian lifestyles as much as possible during the operation, then the answer is "no." If the aim is to contain war's destructiveness and to facilitate restoration of civil society after the conflict, then the answer is "quite probably yes."

IV. A Model Protocol and Conclusions

To announce the, fact that the laws of war continue to apply, an international legal convention guiding the conduct of information operations would be valuable. Rather than creating new rules, however, it would work best if it merely codified customary international law and applied some of the facts to the existing constraints on warfare.[85] Such a protocol might read in relevant part:

> *1. In deciding whether and how to undertake military information operations, each Party agrees to balance the principles of (a) military necessity, (b) proportionality and (c) discrimination....*
>
> *In discriminating between military objectives and impermissible targets, each Party agrees to balance humanity, chivalry, and the likelihood that the objectives could be achieved without physical destruction.*
>
> *2. Ratification of this convention should also confer compulsory jurisdiction to the International Criminal Court [ICC), and failing that to ad hoc international or regional courts vested with appropriate jurisdiction.*

Potential problems with such a proposal are rife, but these problems are not insurmountable and should be overcome. First, the proposed protocol would apply only to state parties, in an era when many transnational aggressors are not states. On the other hand, currently most humanitarian law applies only to states. States remain the fundamental unit of the international system. As non-governmental organizations and groups gain political and legal recognition in the global (i.e. not merely "international") system, then they too can sign and become parties. In any case, this protocol, like Protocol 1, would protect non-state actors as well as state parties.

Second, the proposed protocol lacks a definition of an information operation. However, instead of defining "military information operations," the ICC could build a case law that would allow for more flexible, fact- and context-sensitive interpretations. Because states voluntarily submit to a court's jurisdiction, they could opt out if the case law develops unfairly or in a way that they find disagreeable. That would not, however, halt the creation of new customary international law and eventually *jus cogens*. Should the day come when people can agree upon a definition, it could be added by judicial interpretation, in a dispute or in an advisory opinion.

Third, evidence problems if a case comes before the ICC will be tremendous. However, this may compel those who undertake information operations to document their efforts to fight fairly. Such a requirement will reinforce caution. In addition, computer systems for tracing and tracking a user's keystrokes are increasingly capable - a trend likely to continue as long as commercial users can profit from research about their customers.

Fourth, the principles of humanity and chivalry are very difficult to judge as between societies of different cultures. This problem is central to the laws of war in general. However, inter-societal conflict frequently involves problems of cultural insensitivity; this is not an argument for abandoning efforts to generate and encourage global norms constraining conflict.

Finally, the model protocol does not mention a duty on the part of the defender to segregate military from non-military objectives. Acknowledging the insurmountable economic obstacles to creating redundant military infrastructure, this convention would shift most of the burden of discriminating to the attacker. This might well result in hindering the development of IW capabilities -- a reasonable outcome. On the other hand, the court would have the discretion to decide when the defender unjustly placed its civilians or civilian infrastructure in harm's way.

Discrimination remains critical to the legitimate use of force in the information age. LOAC is facing some of its greatest challenges in keeping UP with the astounding technological changes occurring as information computational, communication and storage capacities double every year or two. In the short run alone, it presents as many challenges as LOAC has ever faced. In the long-run it faces changes in the nature of warfare more dramatic than any in the past two millennia. Still, the principles of military necessity, humanity, and chivalry provide valuable limitations. Diligent, creative, and intelligent application of these principles should see LOAC well into the twenty-first century. An IW protocol and resort to the ICC should help.

As one of the critical revolutions in military technology, information warfare provides a useful instrument for identifying the larger issues that confront military theorists, legal experts, and policymakers. Information warfare is one of the more mature of these new technologies, and therefore is the harbinger of the problems that technology creates for the legal community. This study illuminates the growing gap that exists between the effect on technology on warfare and the laws that govern warfare.

Glossary

AFB	USAF Air Force Base
APC	Armored Personnel Carrier
ARPANET	DOD's Advanced Research Projects Agency-funded progenitor to the internet.
CENTCOM	Central Command
COMPUSEC	Computer Security
C	Command, Control, and Communications
CIA	Central Intelligence Agency
DISA	DOD Defense Information Systems Agency
DOD	Department of Defense
EMP	Electro-magnetic pulse (used in this essay to refer to non-nuclear explosion created EMP)
FBI	Federal Bureau of Investigation
GA	United Nations General Assembly
ICC	International Criminal Court
ICRC	International Committee of the Red Cross
I.L.M.	International Legal Materials, American Society of International Law
IW	Information Warfare
JAG	Judge Advocate General
KGB	Komitet Gosudarstvennoy Bezopastnosti (Committee for State Security, USSR)
LOAC	Law of Armed Conflict
NRC	National Research Council
NSA	NationalSecurity Agency
PCCIP	President's Commission on Critical Infrastructure Protection
RF	radio frequency
SAIC	Science Applications International Corporation
SIGINT	Signals Intelligence -- information derived from intercepting electromagnetic (radio) waves.
U.N.T.S	United Nations Treaty Series
USA	United States Army
USAF	United States Air Force
USN	United States Navy

Appendix I Types of Warfare

	Offensive-Defense	Defensive-Defense	Security (strictly defensive)
Land War	Desert Storm	Desert Shield	Perimeter lookouts; sentries
Naval War	Landing at Normandy	Coastal defense	Sentries looking for saboteurs or mines
IW	Destroy C^3 systems	Destroy an attaching computer	Fire-wlls

Notes

1. In 1995-1996, 1 served as a professor at the Air War College, United States Air Force's senior service school. However, this essay is not directly informed by any classified information, nor does it represent anyone's opinions but my own. All rights reserved. I would like to thank Jonathan Bush, William Martel, W. Darrell Phillips, and Matthew Waxman for their thoughtful comments on previous drafts of this essay. This essay is dedicated to the memory of Brig. Gen. Telford Taylor.

2. Carl von Clausewitz, On War (Michael Howard and Peter Paret, ed., and trans., 1976)(1832) 75. Likewise, centuries before Cicero claimed that inter arma silent leges (in war the law is silent).

3. Telford Taylor, Nuremberg and Vietnam: A n A mericoz Tragedy (1970) 19-20.

4. See, Michael Howard, Introduction, in Michael Howard, George Andreopoulos, and Mark R. Shulman, eds., The Laws of War. Constraints on Wad@am in the Western World (I 994) 2. While the formal laws of war were less developed in the Napoleonic era than they are today, Howard notes that Clausewitz "knew perfectly well ... that the conduct of war was subject to considerably greater and more perceptible limitations in his own time than it had been in the days of, say, Genghis Khan." See also Leslie C. Green, "The Law of War in Historical Perspective" in The Law of Militwy Openitions (Michael N. Schmit@ ed., 1998).

5. Ober, Classical Greek Times, in Howard, Laws of War at 13 ff.

6. Adam Roberts and Richard Guelff, Docwnenu on tlw Laws of War (second edition, 1989) 5 .

7. For an introduction to the notion of the immunity of non-combatants, see Howard, Constraints on Warfare, in Howard, Laws of War, supra n. 4 at 3 ff. Examples of this principle abound in history. For examples, see Robert Stacey, Age of Chivalry, in Id. at 29-3 1; Geoffrey Parker, Early Modern Europe, in Id. at 41, 46; and Gunther Rothenberg, Age of Napoleon, in Id. at 87 ff.

8. For the most horrifying example of this, see David Alan Rosenberg, "Nuclear War Planning" in Id. or Rosenberg. "The Origins of Overkill, Nuclear Weapons and American Strategy, 1945-1960," 7 International Security at 3-71 (Spring 1983).

9. The most interesting inquiry into the end of formal war may be Martin van Creveld, Transformation of War (I 99 1). See also, Paul Kennedy and George J. Andreopoulos, Laws of War.- Some Concluding Reflections, in Howard, Laws of War, supra n. 4 at 214-225.

10. 1928 General Treaty For the Renunciation of War as an Instrument of National Policy ("Kellogg-Briand Pace') T.S. No. 796; and especially 1945 Charter of the United Nations, T.S. No. 993, articles 2(4) ("All members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations") and 51 ("Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations").

11. Roberts and Guelff, supra n. 6 at 1.

12. For the transition, see, Marc L. Warren, Operational Law -A Concept Matures, 152 Mil. L. Rev. 33, 35 (1997)("Military operations other than war present numerous and diverse legal issues.") The formal LOAC began with the field manual Columbia professor Francis Lieber wrote for the Union Army during the Civil War, U.S. Army General Order No. 100, Instructions for the Government of Armies of the United States in the Field. Howard, Laws of War, supng@ n. 4 at 6. General Order No. 100 has undergone significant revisions but remains the basic Field Manual of the U.S. Army, FM 100-5. "Although such national manuals also have a function in providing evidence of the law, they are in general bound to be viewed with some caution." Roberts and Guelff, Laws of War, supra n. 6 at 7.

13. For the former, see International Committee of the Red Cross (ICRC), Final Act of the Diplomatic Conference on the Reaffirmation and Development of International Humanitarian Law Applicable in Armed Conflict(1977).The ICRC was founded at the 1863 Geneva International Conference "with the express purpose of reducing the horror or warfare." Roberts and Guelff, Laws of War, supra n. 6 at 8. For the latter term, see Warren, Operational Law, supra n. 7, 36 ("that body of law, both domestic and international, impacting upon legal issues associated with the planning for and deployment of US Forces overseas in both peacetime and combat environments."); David E. Graham, Operational Law [OPLA WI - A Concept Comes of Age, Army Law., Jul. 1987, at 9.

14. Roberts and Guelff note the "cardinal principle that jus in bello applies in cases of armed conflict whether the conflict is lawful or unlawful in its inception under jus ad bellum." Roberts and Guelff, Laws of War, supra n. 6 at 1.

15. These hypotheticals are based directly on those in Douglas Waller, Onward Cyber Soldiers, Time, (Aug. 21, 1995) [38-44]. See also, (Lt. Col.) Kurt C. Reitinger, New Tools for New Jobs, 124 Proceedings of the U.S. Naval Institute 37 (April 1998) (discussing the need for new doctrine to successfully employ new non-lethal military technology). See also, Elaine Scany, The Fall of TWA 800, The Possibility of Electromagnetic Interference, N. Y. Rev. of Books, April 9,1998.

16. For context on jus ad bellum [just war theory], see Michael Walzer, Just and Unjust Wars (1977) part two. The most critical and difficult jus ad bellum issues for IW include: 1) problems of proof when a party suspects an information assault, and 2) deciding when such an assault attains the level of an "armed attack" as required under UN Charter, art. 51 or "aggression" as defined by the UN General Assembly, G.A. Res. 3314, U.N. GAOR, 29th Sess., Supp. No. 3 1, art. 1, U.N. Doc. 1/9631 (1974). For a start, see, George 1. Seffers and Mark Walsh, Does a Cyber Attack Constitute War? Defense News (Sept. 8, 1997) 1. A recent article does address some of the larger international legal implications, Sean P. Kanuck, Information Warfare: New Challenges for Public International Law 37 Harv. Int'l L.J. 272 (1996)(arguing that successful resolution of international conflicts in the information age will require a new theoretical structure of law).

17. For instance, the U.S. Army has long had a standing capability to engage in psychological operations such as those relying on broadcast reports or distributing pamphlets to encourage an enemy to retire from the field. (Army Chief of Staff, General) Gordon R. Sullivan and (Colonel) James M. Dubik, War in the Information Age, 74 Military Review (Jul. 1993) 46. The Navy also has considerable expertise. See (Vice Admiral) Cebrowski and Gartska, Network-Centric Warfare, infra, n. 20. But the Air Force has an Information Warfare squadron at Shaw AFB, NC. See, USAF JAG School, Legal Aspects, infra n. 25, Appendix F "Principal DoD Information Warfare Organizations" at F-33-34. The USAF also has an Information Warfare Center at Kelly, AFB, TX. The commander, Col. James Massaro, states "[I]nformation superiority - like air superiority - has been declared a core competency by the Air Force." 5 C41 News, no 4, (Aug. 14, 1997). The global nature of IW, makes it unlikely that there will be a

territorial division between domestic and foreign TW as exists in counter-espionage, where the FBI pursues spies domestically and the CIA has responsibility for spies abroad.

18. Dep't of the Air Force (USAF), The Cornerstones of Information Wad@2m 3-4 (1995). Or see Office of the Chief of Naval Operations, Dept' of the Navy, OPNAVINST 3430.26 1 (Jan. 18. 1995) "[A]ction taken in support of national security strategy to seize and maintain a decisive advantage by attacking an adversary's information infrastructure through exploitation, denial, and influence, while protecting friendly information systems."

'Me literature on IW is small but growing and includes: Stuart J.D. Schwartzstein Ed., The Information Revolution and National Security (1996); Winn Schwartau, Information Warfare: Chaos on the Electronic Superhighway (1994); National Research Council (NRC)'s System Security Committee, Computers at Risk: Safe Computing in the Information Age (1991); Alan D. Campen ed., The First Information War (1992); Manuel DeLanda, War in the Age of Intelligent Machines (I 99 1); Kenneth C. Allard, Command, Control, and the Common Defense (1996); Paul Strassmann, The Politics of Information Management (1995); Martin C. Libicki, The Mesh and the Net: Speculations on Armed Conflict in a Time of Free Silicon (1995); David F. Ronfeldt, Cyberocracy, Cyberspace, and Cyberology: Political Effects of the Information Revolution (1991); Gerald Hust, Taking Down Telecommunications (1994); Barry R. Schneider and Lawrence E. Grinter, Battlefield of the Future (1995).

The periodical literature includes: John Arquilla and David Ronfeldt, Cybenvar is Coming, Comparative Strategy (April-June, 1993); Martin C. Libicki and James A. Hazlett, Do We Need an Information Corps? Joint Force Quarterly (Autumn, 1993); P.C. F-nimett, Software Wad'@2m: The Emerging Future, Royal United Services Institute Journal (Dec. 1992); Mary Fitzgerald, Russian Views of Electronic Signals and Information Warfare, American Intelligence Journal. (Spring-Summer 1994); John Rothrock, Information Warfare: Time for some Constructive Skepticism, American Intelligence Journal (Spring-Summer 1994); Craig Johnson, Information War -- Not a Paper War, Journal of

Electronic Defense (August 1994); Chet and Janet Morris and Thomas Barnes, Weapons of Mass Protection: Nonlethality, Information, Warfare, and Airpower in the Age of Chaos, George J. Stein, Information Warfare, and Richard Szaftanski, A Theory of Information Wad@2re: Preparing for 2020, all three in AirPower Journal (Spring, 1995). Richard Szafranski, When Waves Collide: Future Conflict, Joint Forces Quarterly (Spring 1995); Jim Anderson, Chugging up the Onn7mp of the Info Interstate, Foreign Service Journal (March 1995); Defense Technology Economist, (10 June 1995, supplement 5-20); Donald E. Ryan, Implications of Information-Based Warfare, Joint Forces Quarterly (Autumn-Winter 1994-5); H.D. Arnold, J. Hukill, 1. Kennedy, and A. Cameron, Targeting Financial Systems as Centers of Gravity: 'Low Intensity' to 'No Intensity' Conflict, Defense Analysis (v. 10. no., 2, 1994); and Spacceast 2020, Leveraging the Infosphere: Surveillance and Reconnaissance in 2020, Airpower Journal (Summer 1995).

19. The USAF defines information attack as "[dlirectly corrupting information without visibly changing the physical entity within which it resides." Cornerstones, supra 12 at 3-4.

20. The information age is most famously explained by the Toffiers. Alvin Toffler and Heidi Toffler, War and Anti-War.- Survival at the Dawn of the 2]s' Century (1993)(the emerging knowledge-based society will use knowledge-based systems to conduct warfare). See also Mark R. Shulman, WarandA nti-War, 121 Proceedings of the U.S. Naval Institute 84 (October 1994)(book review).

For an overview of information superiority, see Arthur K. Cebrowski and John J. Gartska, Network-Centric Wad@2re Its Origin and Future, 124 Proceedings of the U.S. Naval Institute 88 (January 1998)

28-35; and "The Emerging Joint Strategy for Information Superiority," US DOD, Joint Staff J-6, information briefing at http:llwww.dtic.nii]/JCS/J6.

21. UN Charter, art. 51.

22. Throughout most of the nineteenth century, coastal defense boats and fortresses provided the United States with defensive-defense. As they evolved in the 1880's and 1890's, battleships provided a new offensive-defense, defending the nation instead by threatening to bring the battle to the enemy. Strictly defensive measures were never abandoned; if a spy attempted to destroy a naval vessel in a U.S. harbor, he would have been arrested or killed. See Mark R. Shulman, Navalism and the Emergence of American Sea Power, 1882-1893 (1995) 1-2. For a graphic explanation of these types of warfare, see Appendix.

23. There are potential military applications for information operations that are neither offensive nor defensive. Consider, for instance, the use of radio jamming when Hutu extremists are broadcasting "lists of enemies to be hunted down and butchered." Jamie F. Metzl, Information Intervention, Foreign Affairs (Nov./Dec. 1997) 15-20. See also the more extensive treatment, Jamie F. Metzl, Rwandan Genocide and the International Law of Radio Jamming, 91 American Journal of International Law 628 (1997)(proposing "a narrow exception to general international standard supporting the free flow of information for cases of incitement to genocide or mass human rights abuse."). For a comprehensive program, see, Carnegie Commission on Preventing Deadly Conflict, Final Report: Preventing Deadly Conflict, (1997). See also, Warren, Operational Law, supra n. 7 at 34-37 and Joint Chiefs of Staff Publication 307, Joint Doctrine for Military Operations other Than War

24. Active gathering would include such measures as infiltrating another country's computer systems, either by sitting down in front of its dedicated terminals or via telecommunications systems from a distance. Compare to passive gathering, which includes such measures as intercepting broadcasted communications.

25.This list is suggested by Col Phillip A. Johnson, USAF, Associate Deputy General Counsel (IA), Office of the General Counsel, DOD, in "Opening Shots: Information Warfare and the Law," brief to FY 98 Legal Aspects of Information Operations Symposium, Air Force Judge Advocate General School, Maxwell, AFB, AL.

Another more comprehensive list proposes that offensive-defense operations could include: "psychological operations, military deception, jamming of enemy information systems, signal intelligence (SIGRM, and attacks on enemy information systems by physical destruction or by electronic means." Primer on Legal Issues in Information Operations (3rd edition)(draft, October 1997), 13-14. Note that both lists come from the USAF indicating not confusion but an ever-changing reality.

26. For a more complete discussion of the war powers, see Louis Henkin, The Use of Force: Law and U.S. Policy, in Right v. Might: International Law and the Use of Force (Council on Foreign Relations, 2nd edition, 199 1). For operations conducted by intelligence services, see Roy Godson, Dirty Tricks or Trump Cards: U.S. Covert Action and Counterintelligence (1995); W. Michael Reisman and James Baker, Regulating Coven Action: Practices, Contexts, and Politics of Covert Coercion Abroad in International and American Law (I 992); Robert F. Turner, Coercive Court Action and the Law Regulating Covert Action, 20 Yale Journal of International Law 427 (book review)(1995).

27. National Security Act of 1947, 50 U.S.C. §§403, 413 (1982); The Foreign Assistance Act of 1961 §662, 22 U.S.C. 2422 (1988).

28. Exec. Order No. 12,333. Emphasis added. Section 1. I I (e) also provides that the secretary of defense shall "Conduct programs and missions necessary to fulfill national, departmental, and tactical foreign intelligence requirements."

29. Reisman and Baker, Regulating Covert Action, supra n. 26 at 119. At the time of publication, Baker was Attorney Advisor in the Office of Legal Counsel, Department of State. He should not be confused with the then Secretary of State.

30. These restraints now include most famously and substantively, a ban on assassination. This ban presents an irony by barring excessive discrimination. President Gerald Ford issued an executive order to ban U.S. intelligence officers from "engag[ing] in, or conspir[ing] to engage in, political assassination." Executive Order 11,905, "United States Foreign Intelligence Activities," February 18, 1976, § 5(g) [41 Fed. Reg. 7,733 (1976)). President Jimmy Carter issued Executive Order 12,036, Jan. 24, 1978, §2-305 [43 Fed. Reg. 3687] and President Ronald Reagan issued Executive Order 12,333, Dec. 4,1981, §2.11 [48 Fed. Reg. 59,947 (1981)]. See, Abram N. Shutsky, Silent Warfare: Understanding the Intelligence World (2nd edition, rev. Gary J. Schmitt, 1993) 100-101.

The debate, however, is not over. See Reisman and Baker Regulating Covert Action, supra n. 26 at 71; Robert F. Turner, Killing Saddam: Would it be a Crime? Washington Post, Oct. 7, 1990, at D1 (commentary and opinion); (LCDR) Bruce A. Ross, The Case for Targeting Leadership in War, 46 Naval War College Review 73; and George Stephanopoulos, Why We Should Kill Saddam, Newseek (Dec. 1, 1997) at 34. Turner, Ross, and Stephanopoulos argue that the ban forces the U.S. to invade a country like Panama (or potentially Iraq) at great risk and cost rather than effecting a more efficient solution.

31. Primer, supra n. 25 at 41.

32. A clipper chip is the proposed electronic processor that would allow authorized key-holders to decrypt a encrypted transmission, one in which mathematical algorithms are used to "scramble data to protect its confidentiality." See, Scott Sharney and Kent Alexander, Computer Crime, [45] Emory L. J. 931 (1996) 93. In theory the chip could be added to a machine built almost anywhere by anyone, but it would likely be simpler to add to machines manufactured in the United States.

33. Some American teenagers pose relatively serious threats, but they are subject to criminal law and retain constitutional protections. See, for example, United States v. Morris, 928 F.2d 504 (2d Cir. 1991) (young American hacker inserted a worm -- a self-contained computer program -- into various computers via the Internet that crippled 6,200 computers and caused nearly 100 million dollars in damage). Alternatively an apparently harmless hacker may be in the employ of an unfriendly foreign intelligence service and capable of inflicting serious harm. See Clifford Stoll, The Cuckoo's Egg (1989) (young German in employ of KGB hacked into US defense-related computers). And see Charney and Alexander, supra n. 32, at 931. See also M. E. Bowman, Is International Law Ready for the Information Age? 19 Fordham Int'l L. J. 1935 (1996) (author as Associate General Counsel of the FBI is concerned with attacks on National Information Infrastructure [NII]).

34. CENTCOM is the unified operational command responsible for U.S. military forces in the Middle East and the Indian Ocean basin.

35. Graeme Browning, Hack Attacks, Government Executive (Aug. 1977) 23.

36. Robert t. Marsh, Chairman, PCCIP, Remarks Prepared for Delivery, "The Role of Government in the 21st Century," (Sept. 20, 1997) http://www/pccip.gov/marsh_kennedy.html. ("The General Accounting Office reported that DoD's computers were the target of approximately 250,000 intrusions last year. Even more troubling, only a small percentage of these are detected and even fewer are reported.") as a test of 9,000 DOD computer networks, the Defense Information Systems Agency (DISA) hacked into and took control of 88 percent of the networks. Only 4 percent of systems operators recognized that they had lost control and only 0.2 percent reported the events. 21-Fall Fletcher Forum of World Affairs, infra n. 44 at 83-84. See also, John Elvin, "Insight" Washington Times (March 23, 1998) p. 32.

37. Primer, supra n. 25 at 8.

38. Richard B. Lillich, Forcible Self-Help Under International Law, in National Security Law 131, 132-33 (John Norton Moore et al., 1990) 130. Or see, Louis Henkin, et al, International Law: Cases and Materials 579 (3rd ed. 1993)("Retorsion is often an 'equivalent' act of retaliation in response to an unfriendly act.")

39. Lillich, supm n. 32 at 133.

40. Moreover, a vast literature debates whether the UN Charter bans retorsion and reprisals as impermissible uses of force. UN Charter, Art. 2(4). Lillich summarizes the debate, Id. at 133-36. As long as the response is limited to non-forceful measures such as using computer code to neutralize the offending machinery, this issue should be avoidable. Lillich concludes the discussion by summarizing a speech by Professor Myres McDougal on how to read Art. 2(4), "in the absence of collective machinery to protect people against attack and deprivation... the principle of major purposes requires an interpretation which would honor self-help against a prior unlawfulness." Id. at 136.

41. Primer, supra n. 25 at 8. An intruder might enter through a "trap door" of his own creation. He may gain initial entry through a Trojan Horse -a program which on its face has a legitimate purpose but has a hidden, illicit purpose. Note the term's origins in a ruse of war.

42. Browning, Hack Attack, supra n. 24 at 23.

43. Chamey and Alexander, supra n. 32 at 936-937. See, NRC, Computers at Risk supra n. 72; Emilio Jaksetic, Computer Security and Government Lawyers, Fed. Law. (Jul. I996) 1.

44. President's Commission on Critical Infrastructure Protection (PCCIP), Overview Briefing, F-3 (June 1997) http:/Iwww/pceip.govi. See also, Greg Rattray, The Emerging @Global Infrastructure and National Security, 21 -Fall Fletcher For-um of World Affairs 8 1. But see, Marc D. Goodman, Why the Police Don't Care About Computer Crime, 1O Harvard Journal of Law and Technology. 465 (1997).

45. Executive Order 13,010, cited in PCCIP, Overview Briefing, F-3.

46. For these citations, the author is indebted to Major Stanley R. Smith's briefing on hacker law, before the Legal Aspects of Information Warfare Symposium, Air Force Judge Advocate General School, Maxwell AFB, AL (1-3 November 1995). For a more complete listing of relevant U.S. law, see Science Applications International Corporation (SA IC) Telecommunications and Networking Systems Operation,

Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance (1995), app. B, "United States Code: Annotated Bibliography and Index." Table 2-2-1 of this report enumerates the various state computer crime statutes.

47.1d., table2-2-2indicatesthevariousjurisdictionsforComputerCrimesthatoccur in this country. If an intruder penetrates a Federal system in the U.S. with criminal intent, the act falls under the jurisdiction of the FBI and the U.S. Secret Service. If the intent were espionage, then the FBI shares jurisdiction with the National Security Agency.

48. "In view of the large number of states parties to the 1949 Geneva Conventions and the status which the Conventions have acquired in the international community, it is reasonable to assume that the Conventions are (at least in large part) declaratory of customary international law." Roberts and Guelff, Documents on the Laws of War, infra n. 6 at 170. See also the War Crimes Act of 1996, 18 U.S.C. chapter 118, §2401.

The 1949 Geneva Conventions are comprised of. (1) Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, opened for signature Aug. 12, 1949, 6 U.S.T. 3114, 75 U.N.T.S. 3 1; (2) Geneva Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea, opened for signature Aug. 12,1949,6 U.S.T. 3217,75 U.N.T.S. 85; (3) Geneva Convention Relative to the Treatment of Prisoners of War, opened for signature Aug. 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 135; (4) Geneva Convention Relative to the Protection of Civilian Persons in Time of War, opened for signature Aug. 12, 1949, 6 U.S.T. 3516, 75 U.N.T.S. 287 [hereinafter Geneva Convention IV].

See also, 1968 United Nations General Assembly Resolution 2444, "Respect for Human Rights in Armed Conflicts" affirming these general principles: (a) That the right of the parties to a conflict to adopt means of injuring the enemy is not unlimited; (b) That it is prohibited to launch attacks against the civilian populations as such; and (e) That distinction must be made at all times between persons taking part in the hostilities and members of the civilian population to the effect that the latter be spared as much as possible.

49. Protocol Addition to the Geneva Conventions of 12 August 1949, and Relating the Protection of Victims of International Armed Conflicts (Protocol 1), art. 48. 1125 U.N.T.S. (I 979)[hereinafter Protocol 11. "Although the U.S. miliftry takes the position that an attacker should accept some responsibility to minimize collateral civilian casualties" the United States has not ratified Protocol I because it shifts the burden to segregate civilians from military objectives to the attacker from its traditional situation where the defender carried this obligation. Danielle L. Infeld, Note, Precision-guided munitions demonstrated their pinpoint accuracy in desert storm; but is a country obligated to use precision technology to minimize collateral civilian injury and damage? 26 GW J. Int'l L. and Econ. 109 (1992) at 122-123. See also Howard Levie, The 1977 Protocol I and the United States, 38 St. Louis U. L.J. 469 (1993) reprinted in, Levie on the Law of War (Michael N. Schmitt and Leslie C. Green, eds. 1998)(arguing that the United States should ratify the protocol). See also Horace B. Robertson, Jr. The Principle of the Military Objective in the Law of Armed Conflict in The Law of Military Operations, supra note 4.

50. Protocol 1, art. 51.

51. "The International Court of Justice (ICJ) at The Hague has long had certain limited roles in respect of implementation of the laws of war... [but its] statute, with its built-in limitations on what types of cases may be brought to it and by whom, is likely to mean that it only will have to look at a minority of issues

concerning the laws of war." Adam Roberts, The Laws of War.- Problems of Implementation in Contemporary Conflicts 6 Duke Journal of Comparative and International Law 11 at 43. Legal Constraints on Information Wad@7m ... 31

52. International Court of Justice, Advisory Opinion on the Legality of the Threat or Use of Nuclear Weapons, 35 I.L.M. (1996) 809. See also, Robert F. Turner, Nuclear Weapons and the World Court: The ICJs Advisory Opinion and Its Significance for U.S. Strategic Doctrine " in The Law of Military Operations, supra note 4.

53. Protocol 1, art. 43.

54. Protocol 1, art. 52(2). The definition is emphasized by the U.S. Navy. See, Commander's Handbook (Supp.) supra n. 49 at 8.1.1 (1989).

55. Distinguishing civilians from military personnel has traditionally been a matter of recognizing the military professionalism which has organized the officer corps of the western powers since the early nineteenth century, Samuel Huntington, Soldier and the State (1957). Still uniformed soldiers fighting others organized into particular standing units that had trained and been armed together goes back to at least the end of the Thirty Years War when rulers and people alike recoiled from the horror of unbridled warfare where distinctions between combatants and noncombatants had disintegrated. Michael Howard, Constraints on Warfare, Laws of War, supra n. 4 at 4 ("[T]he nightmare days of the Thirty Years War when troops, themselves desperate and starving, tortured, slaughtered, and burned their way across Europe were not prolonged into the following century"). See also Howard's classic, War in European History (I 976).

56. Technically this has been true only for professional or conscription armies. The combatants of the colonized world (i.e. the indigenous peoples of the Americas, Africa, Asia and the Pacific) did not usually wear recognizable uniforms. This cultural difference between the imperial powers and the colonized world only fed the cultural, religious, geopolitical, and economic forces that undermined the constraints on warfare when it was between cultures. That is to say, the restraints on the western way of war usually did not apply in conflicts between Western Europeans and the rest of the world. See, Howard, in Laws of War, supra n. 4.

57. See Taini Davis Biddle, Air Power and David Alan Rosenberg, Nuclear War Planning, in Laws of War supra n. 4. See generally W. Hays Parks, Air War and the Law of War, 32 A.F. L. Rev. 1, 89-168 (1990). During the inter-war period, the 1923 Hague Draft Rules of Aerial Warfare "were regarded as an authoritative attempt to clarify and formulate the rules of air warfare." Roberts and Guelff, Laws of War, supTI4 no. 6 at 121.

58. "Customary law is found in the practice of states, how many is not precisely stated, ... which is binding upon all persons of international law irrespective of treaty commitments." Hilaire McCoubrey, International Humanitarian Law: The Regulation of Armed Conflicts 192 (1990). The United Stat4s is bound by customary international law. Restatement (Third) of Foreign Relations Law of the United States § 102; Louis Henkin, International Law as Law in the UnitedStates, 82 Michigan Law Review. 1555 (1984).These three principles are also used for determining proportionality.

59. U.S. Dep't of Defense, DOD Law of War Program, DOD Directive 5100.77 (1979). See also Almond, The Teaching and Dissemination of the Geneva Conventions and International Humanitarian Law in the United States, 31 Am. U. L. Rev. 981 (1982). Nonetheless, when I taught at the Air War

College in 1995-1996, fulfilment of this requirement seemed to have lapsed from the core curriculum. When I pointed this out, a leading JAG lawyer was brought in for a mandatory lecture. Apparently, since I left, the War College has allowed this program to lapse again.

60. Geneva Convention IV, art. 53. See also, Office of the Judge Advocate General, Dep't of the Navy, Annotated Supplement to the Commander's Handbook on the Law of Naval Operations, 5.2 (1989) cited in Walter Gary Sharp, Sr., Cyberspace and the Use of Force: Information Operations, the Laws of War and the United States Standing Rules of Engagement, L-13.

61. Preamble, 1907 Hague Convention (IV) Respecting the Laws and Customs of War on Land, Signed Oct. 18, 1907, entered into force Jan. 26, 1910 [hereinafter Hague IV]. Emphasis added.

62. 1949 Geneva Convention 1, Art. 63; Convention U, Art. 62; Convention Ell, Art. 142; and Convention IV, Art. 158. Emphasis added. This principle was likewise confirmed by the 1977 Geneva Protocol 1, art. 1; 1977 Geneva Protocol R, Preamble; and 1981 UN Weapons Convention, Preamble. See Roberts and Guelff, Laws of War, supra n. 6, at 4 and note 8.

63. See, Commander's Handbook (Supp.) supra n. 49 at 5.2; Air Force Judge Advocate School, The Military Commander and the Law (I 994) 580.

64. Herrnan Hathaway and Archer Jones, How the North Won (1983) at 548. While U.S. Civil War general William T. Sherman is renowned for having made a military strategy of this notion, he is far from alone in history. See, for example, Harold Selesky, Colonial America, in Howard, Laws of War, supm n. 4 at 61 (the British conquerors of Ireland justified their atrocities as expedient); Biddle, A irpower, in Id., at 147, n 23,ff (strategic air power theorists believed that bombing civilians would destabilize the enemy society and economy, eventually toppling the state). Even the vaunted Lieber Code includes a strand of this now-outlawed logic. Lieber Code, supra n. 12, art., XXXIX ("the more vigorously wars are pursued, the better it is for humanity. Sharp wars are brief.")

65. See for instance, The International Covenant on Civil and Political Rights, art. 2. 1, 999 U.N.T.S. 17 1; International Covenant on Economic, Social and Cultural Rights, art. 2.2., 993 U.N.T.S. 3; or Convention on the Elimination of A 11 Forms of Discrimination Against Women, G.A. Res. 180 (XXXIV 1979).

66. Protocol 1, art. 37. For the obligations of chivalry, see also United States, Department of the Navy, Office of the Chief of Naval Operations, The Commander's Handbook on the Law of Naval Operations, NWP 9, Washington, DC, (1987) at 5- 1, as cited in Roberts and Guelff, Laws of War, supra n. 6 at 5, note I 1.

67. Protocol 1, art. 37 § § 1-2; Hague IV, art. 24. See also, Military Commander a& the Law, supra n. 63 at 581.

68. Edward N. Luttwak, Toward Post-Heroic Warfare, Foreign Affairs (May/June 1995).

69. A logic bomb would function like a virus that could selectively degrade or even destroy the computer hosting it. Protocol 1, art. 38; see also Primer supra n. 25 at 17-18; Richard Aldrich, The International Legal Implications of Information Warfare, Airpower J. (Fall 1996) at 108.

70. Hague Convention IV, art. 29 states "A person can only be considered a spy when, acting clandestinely or on false pretenses, he obtains or endeavours to obtain information in the zone of operations of a belligerent, with the intention of communicating it to the hostile party." Article 30 requires merely that a "spy taken in the act shall not be punished without previous trial." The Geneva Convention IV, Part 1, art. 5 governing suspected spies in occupied territory merely requires a fair trial.

71. Hague Convention IV, art. 3 1. 72. Id., art. 22.

73. Hague Convention TV, art 27. Because these provisions failed to protect cultural property in World War 11, a stronger convention was sought by the international community. The result was the 1954 Hague convention for the Protection of Cultural Property in the Event of Armed Conflict, signed May 14,1954 and entered into force on Aug. 7,1956,249 U.N.T.S. 240-88 [hereinafter 1954 Hague Conv.]. The principles it embodies were most recently affirmed in Protocol 1, art. 53 and Article 16 of Geneva Protocol 11. This "special protection may be viewed as part of customary international law." Roberts and Guelff, Laws of War, supra n. 6 at 340.

74. 1954 Hague Conv. at 240. To receive this protection, however, cultural property must be "situated at an adequate distance from any large industrial centre or from any important military objective constituting a vulnerable point... and cannot be used for military purposes." 1954 Hague Conv. § 8(l)(a)-(b), 249 U.N@.T.S. at 246.

75. Iraq purposefully located legitimate military targets near its civilian population, civilian objects, and cultural property. U.S. Dep't of Defense, Conduct of the Persian Gulf War. Final Report to Congress 125-26 (1992) app. 0, at 0-14. Infeld, Precision-guided munitions, supra n. 49 at 137.

76. Protocol 1, art 56(t) 1 2 does make limited exceptions for those works being used "for other than (their] normal function and in regular, significant and direct support of military operations and if such attack is the only feasible way to terminate such support."

77. Id., art. 54.

78. Hague Convention IV, art. 25. And see Hague Draft Rules on Aerial War, supra n. 57.

79. "Customary practice has been that military equipment such as units and bases, and economic targets such as power sources, industry, transportation, and command and control centers, are always legitimate targets.... This includes transportation and communications systems.... However, 'the inherent nature of an object is not controlling; its value to the enemy or the perceived value of its destruction is the determinant.' . . . Even traditional civilian objects, such as private homes, if used for military purposes, may be attacked. The important factor is to determine if the target makes an effective contribution to the enemy's military operations; if it does, it is subject to attack, wherever located, even if within heavily populated areas.' See U.S. Dep't of the Air Force, AFP 200-17, A n Introduction to Air Force Targeting 9 (1989)." Infeld, Precision-guided munitions, supra n. 49 at 122 (1992).

80. Protocol 1, art. 44(3). Recall also, Protocol 1, article 48's Basic Rule, "In order to ensure respect for and protection of the civilian population and civilian objects, the Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives.?' Emphasis added to show that the burden falls both on attacker and defender.

81. "Warfare is no longer primarily a function of who puts the most capital labor, and technology on the battlefield, but of who has the best information about the battlefield." Arquilla and Ronfeldt, Cyberwar is Coming! 12 Comparative Strategy 141, 144, (1993).

82. This despite the military origins of the ARPANFT/Internet. Marsh, Remarks, supra n. 36.

83. Writing in an unofficial capacity, Colonel Owen E. Jensen states: "Cut or deny all the enemy's information-transfer media - telephone, radio frequencies (RF), cable, and other means of transmission. Sever the nervous system. Deny, disrupt, degrade, or destroy every transmission." Jensen, Information Warfare: Principles of Third-Wave War, 8 Airpower Journal no. I (Winter 1994) at 37. Presumably Colonel Jensen is not writing as a lawyer. Maj. Richard W. Aldrich, however, does examine the legal issues raised by Jensen's statements. See Aldrich, International Legal Implications, supn7, n. 69 at 105-09.

84. Primer, supra n. 25 at 18.

85. Among others, Robert and Guelff note that "[t]echnological developments in the methods of conducting war have increased the extent to which the written law is inadequate or absent." Roberts and Guelff, Laws of War, supra n 6 at 15.

Center for Strategy and Technology

The Center for Strategy and Technology was established at the Air War College in 1996. Its purpose is to engage in long-term strategic thinking about technology and its implications for U.S. national security.
The Center focuses on education, research, and publications that support the integration of technology into national strategy and policy. Its charter is to support faculty and student research, publish research through books, articles, and occasional papers, fund a regular program of guest speakers, host conferences and symposia on these issues, and engage in collaborative research with U.S. and international academic institutions. As an outside funded activity, the Center enjoys the support of institutions in the strategic, scientific, and technological worlds. Principal funding is provided by the Air Force Research Laboratory (AFRL), with additional support from the Defense Advanced Research Projects Agency (DARPA).
An essential part of this program is to establish relationships with organizations in the Air Force as well as other Defense of Department agencies, and identify potential topics for research projects. Research conducted under the auspices of the Center is published as Occasional Papers and disseminated to senior military and political officials, think tanks, educational institutions, and other interested parties. Through these publications, the Center hopes to promote the integration of technology and strategy in support of U.S. national security objectives.
For further information on the Center on Strategy and Technology, please contact:

William C. Martel, Director
Air War College
325 Chennault Circle
Maxwell AFB Montgomery, AL 36112

(334) 953-2384 (DSN 493-2384)

Email: wmartel@maxl.au.afmil

The Occasional Papers
series was established by the
Center for Strategy and Technology
as a forum for research
on topics that reflect
long-term strategic thinking
about technology and its
implications for
U. S. national security.

Center for Strategy and Technology
Air War College

Maxwell Air Force Base
Montgomery, Al 36112